| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-7** | LEAST FUNCTIONALITY | |
| **CM-7.1**  **CM-7.1.1**  **CM-7.1.1a**  **CM-7.1.1b**  **CM-7.1.1c**  **CM-7.1.1d**  **CM-7.1.2**  **CM-7.1.3**  **CM-7.1.3a**  **CM-7.1.3b**  **CM-7.1.3c**  **CM-7.1.3d** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines for the information system prohibited or restricted:*    * *functions;*    * *ports;*    * *protocols; and*    * *services;* 2. *the organization configures the information system to provide only essential capabilities; and* 3. *the organization configures the information system to specifically prohibit or restrict the use of organization-defined:*    * *functions;*    * *ports;*    * *protocols; and/or*    * *services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Test**: [*select from:* Information system for disabling or restricting functions, ports, protocols, and services]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, RA-5  concurrent controls: AC-2, AC-3, AC-4, AC-6, CM-2, CM-3, CM-5, CM-6, CM-8, SA-7, SC-7  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **CM-7.1.1.1**  **CM-7.1.1.1.a**  **CM-7.1.1.1.b**  **CM-7.1.1.1.c**  **CM-7.1.1.1.d** | | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the list of prohibited or restricted:   * + functions;   + ports;   + protocols; and   + services; |
|  | |  |
| **CM-7.1.2.1** | | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the configurations to be employed in the information system to provide only essential capabilities. |
| **CM-7.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in CM-7.1.2.1; [*reviewing*] for evidence that the information system is configured as identified in CM-7.1.2.1. |
| **CM-7.1.2.3** | | **Test** an agreed-upon [*basic*] sample ofinformation system components; conducting [*basic*] testing for evidence that the information system is configured to provide only essential capabilities. |
|  | |  |
| **CM-7.1.3.1**  **CM-7.1.3.1.a**  **CM-7.1.3.1.b**  **CM-7.1.3.1.c**  **CM-7.1.3.1.d** | | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the configurations to be employed in the information system to prohibit or restrict the use of:   * + functions identified in CM-7.1.1.1.a;   + ports identified in CM-7.1.1.1.b;   + protocols identified in CM-7.1.1.1.c; and/or   + services identified in CM-7.1.1.1.d |
| **CM-7.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in CM-7.1.3.1.a; [*reviewing*] for evidence that the information system is configured as identified in CM-7.1.3.1.a to restrict the use of prohibited or restricted functions. |
| **CM-7.1.3.3** | | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in CM-7.1.3.1.b; [*reviewing*] for evidence that the information system is configured as identified in CM-7.1.3.1.b to restrict the use of prohibited or restricted ports. |
| **CM-7.1.3.4** | | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in CM-7.1.3.1.c; [*reviewing*] for evidence that the information system is configured as identified in CM-7.1.3.1.c to restrict the use of prohibited or restricted protocols. |
| **CM-7.1.3.5** | | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in CM-7.1.3.1.d; [*reviewing*] for evidence that the information system is configured as identified in CM-7.1.3.1.d to restrict the use of prohibited or restricted services. |
| **CM-7.1.3.6** | | **Test** an agreed-upon [*basic*]sample of information system components; conducting [*basic*] testing for evidence that the information system is configured to prohibit or restrict the functions, ports, protocols and services identified in CM-7.1.3.1. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-7(1)** | LEAST FUNCTIONALITY |
| **CM-7(1).1**  **CM-7(1).1.1**  **CM-7(1).1.1a**  **CM7(1).1.1b**  **CM-7(1).1.1c**  **CM-7(1).1.1d**  **CM-7(1).1.2**  **CM-7(1).1.2a**  **CM-7(1).1.2b**  **CM-7(1).1.2c**  **CM7(1).1.2d** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of information system reviews to identify and eliminate unnecessary:*    * *functions;*    * *ports;*    * *protocols; and/or*    * *services; and* 2. *the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary:*    * *functions;*    * *ports;*    * *protocols; and/or*    * *services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, RA-5  concurrent controls: AC-2, AC-3, AC-4, AC-6, CM-2, CM-3, CM-5, CM-6, CM-8, SA-7, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-7(1).1.1.1**  **CM-7(1).1.1.1.a**  **CM-7(1).1.1.1.b**  **CM-7(1).1.1.1.c**  **CM-7(1).1.1.1.d** | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the frequency of conducting information system reviews to identify and eliminate unnecessary:   * + functions;   + ports;   + protocols; and/or   + services. |
|  |  |
| **CM-7(1).1.2.1**  **CM-7(1).1.2.1.a**  **CM-7(1).1.2.1.b**  **CM-7(1).1.2.1.c**  **CM7(1).1.2.1.d** | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to review the information system in accordance with the frequency identified in CM-7(1).1.1.1, to identify and eliminate unnecessary:   * + functions;   + ports;   + protocols; and/or   + services. |
| **CM-7(1).1.2.2** | **Examine** an agreed-upon [*basic*] sample of information system reviews; [*reviewing*] for evidence that the measures identified in CM-7(1).1.2.1 are being applied. |
| **CM-7(1).1.2.3** | **Interview** an agreed-up [*basic*] sample of organization personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system; conducting [*basic*] discussions for further evidence that information system reviews are performed in accordance with the measures identified in CM-7(1).1.2.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-7(2)** | LEAST FUNCTIONALITY |
| **CM-7(2).1**  **CM-7(2).1.1**  **CM-7(2).1.1a**  **CM-7(2).1.1b**  **CM-7(2).1.1c**  **CM-7(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops and maintains one or more of the following specifications to prevent software program execution on the information system:*    * *a list of software programs authorized to execute on the information system;*    * *a list of software programs not authorized to execute on the information system; and/or*    * *rules authorizing the terms and conditions of software program usage on the information system; and* 2. *the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; other relevant documents or records].  **Test:** [*select from:* Automated mechanisms preventing software program execution on the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, RA-5  concurrent controls: AC-2, AC-3, AC-4, AC-6, CM-2, CM-3, CM-5, CM-6, CM-8, SA-7, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-7(2).1.1.1**  **CM-7(2).1.1.1.a**  **CM-7(2).1.1.1.b**  **CM-7(2).1.1.1.c** | **Examine** configuration management policy, procedures addressing specifications to prevent software program execution on the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to develop and maintain one or more of the following specifications to prevent software program execution on the information system:   * + a list of software programs authorized to execute on the information system;   + a list of software programs not authorized to execute on the information system; and/or   + rules authorizing the terms and conditions of software program usage on the information system; and |
| **CM-7(2).1.1.2** | **Examine** list of software programs authorized to execute on the information system and an agreed-upon [*basic*] sample of associated change control records, maintenance records, or information system audit records; [*reviewing*] for evidence that the measures identified in CM-7(2).1.1.1.a are being applied. |
| **CM-7(2).1.1.3** | **Examine** list of software programs not authorized to execute on the information system and an agreed-upon [*basic*] sample of associated change control records, maintenance records, or information system audit records; [*reviewing*] for evidence that the measures identified in CM-7(2).1.1.1.b are being applied |
| **CM-7(2).1.1.4** | **Examine** rules authorizing the terms and conditions of software program usage on the information system and an agreed-upon [*basic*] sample of associated change control records, maintenance records, or information system audit records; [*reviewing*] for evidence that the measures identified in CM-7(2).1.1.1.c are being applied. |
| **CM-7(2).1.1.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for preventing software program execution on the information system; conducting [*basic*] discussions for further evidence that the measures identified in CM-7(2).1.1.1 are being applied. |
|  |  |
| **CM-7(2).1.2.1** | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent software program execution on the information system in accordance with the specifications identified in CM-7(2).1.1.1. |
| **CM-7(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-7(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-7(2).1.2.1. |
| **CM-7(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-7(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-7(3)** | LEAST FUNCTIONALITY |
| **CM-7(3).1**  **CM-7(3).1.1**  **CM-7(3).1.1a**  **CM-7(3).1.1b**  **CM-7(3).1.1c**  **CM-7(3).1.2**  **CM-7(3).1.2a**  **CM-7(3).1.2b**  **CM-7(3).1.2c** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines registration requirements for:*    * *ports;*    * *protocols; and*    * *services; and* 2. *the organization ensures compliance with organization-defined registration requirements for:*    * *ports;*    * *protocols; and*    * *services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, RA-5  concurrent controls: AC-2, AC-3, AC-4, AC-6, CM-2, CM-3, CM-5, CM-6, CM-8, SA-7, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-7(3).1.1.1**  **CM-7(3).1.1.1.a**  **CM-7(3).1.1.1.b**  **CM-7(3).1.1.1.c** | **Examine** configuration management policy, procedures addressing registration requirements for information system component functionality, configuration management plan, or other relevant documents; [*reviewing*] for the registration requirements for:   * + ports;   + protocols; and   + services. |
|  |  |
| **CM-7(3).1.2.1**  **CM-7(3).1.2.1.a**  **CM-7(3).1.2.1.b**  **CM-7(3).1.2.1.c** | **Examine** configuration management policy, procedures addressing registration requirements for information system component functionality, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure compliance with the registration requirements identified in CM-7(3).1.1.1 for:   * + ports;   + protocols; and   + services. |
| **CM-7(3).1.2.2** | **Examine** registration records foran agreed-upon [*basic*] sample of ports, protocols, and services enabled on the information system; [*reviewing*] for evidence that the measures identified in CM-7(3).1.2.1 are being applied. |
| **CM-7(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for establishing and enforcing registration requirements for ports, protocols, and services enabled on the information system; conducting [*basic*] discussions for further evidence that the measures identified in CM-7(3).1.2.1 are being applied. |